

United States District Court

for the
Western District of New York

United States of America

v.

TROY M. MALECKI

Case No. 16-M- 5121



CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about September 18, 2015, in the Western District of New York, the above named defendant did knowingly possess material, that is, an LG-VS980 Cellular Telephone, S/N 990002590723209, produced in the country of Korea, which contained images of child pornography as defined in Title 18, United States Code, Section 2256(8), that involved a prepubescent minor and a minor who had not attained 12 years of age, that had been shipped and transported using any means and facility of interstate and foreign commerce; that had been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer; and that had been produced using materials that had been mailed and shipped and transported in and affecting interstate and foreign commerce by any means, including by computer.

All in violation of Title 18, United States Code, Sections 2252A(a)(5)(B) and 2252A(b)(2).

This Criminal Complaint is based on these facts:

☒ Continued on the attached sheet.

Complainant's signature

Steven Miller, Special Agent
Federal Bureau of Investigation

Printed name and title

Sworn to before me and signed in my presence.

Date: September 26, 2016

Judge's signature

City and State: Buffalo, New York

MICHAEL J. ROEMER
UNITED STATES MAGISTRATE JUDGE

Printed name and title

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

STATE OF NEW YORK)
COUNTY OF ERIE) SS:
CITY OF BUFFALO)

I, **S. R. Miller**, being duly sworn, depose and say:

1. I am a Special Agent with the Federal Bureau of Investigation and entered on duty in 2007. I am currently assigned to the Buffalo Field Office Child Exploitation Task Force, which targets individuals involved in the on-line sexual exploitation of children. I have participated in investigations of persons suspected of violating federal child pornography laws, including Title 18, United States Code, Sections 2251, 2252 and 2252A. I have also participated in various FBI mandated and volunteer training for the investigation and enforcement of federal child pornography laws in which computers are used as the means for receiving, transmitting, and storing child pornography.

2. I make this affidavit in support of a criminal complaint charging **TROY MALECKI**, with violating Title 18, United States Code, Section 2252A(a)(5)(B).

3. The information in this affidavit is based upon my personal knowledge and upon information provided to me by law enforcement officers and others. Because this affidavit is being submitted for the limited purpose of securing a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that **TROY**

MALECKI, hereinafter “the defendant,” did knowingly violate Title 18, United States Code, Section 2252A(a)(5)(B).

4. The defendant has been linked to an online community of individuals who regularly send and receive child pornography via a website that operated on an anonymous online network. The website is described below and referred to herein as “Website A.”¹ There is probable cause to believe that the defendant knowingly possessed, attempted to possess, accessed and/or attempted access with intent to view child pornography on “Website A.”

The Network

5. “Website A” operated on a network (“the Network”) available to Internet users who are aware of its existence. The Network is designed specifically to facilitate anonymous communication over the Internet. In order to access the Network, a user must install computer software that is publicly available, either by downloading software to the user’s existing web browser, downloading free software available from the Network’s administrators, or downloading a publicly-available third-party application.² The software

¹ The actual name of “Website A” is known to law enforcement. Disclosure of the name of the site would potentially alert its members to the fact that law enforcement action is being taken against the site and its users, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the website will be identified as “Website A.”

² Users may also access the Network through so-called “gateways” on the open

prevents someone attempting to monitor an Internet connection from learning what sites a user visits and prevents the sites the user visits from learning the user's physical location by routing communication through other computers. Therefore, traditional IP identification techniques are not viable.

6. "Website A" was located on this Network designed specifically to facilitate anonymous communication over the Internet. Accordingly, "Website A" could not generally be accessed through the traditional Internet.³ Only a user who had installed the appropriate software on the user's computer could access "Website A." Even after connecting to the Network, however, a user had to know the exact web address of "Website A" in order to access it. Websites on the Network are not indexed in the same way as websites on the traditional Internet. So, unlike on the traditional Internet, a user could not simply perform a Google search for the name of "Website A," obtain the web address for "Website A," and click on a link to navigate to "Website A." Rather, a user had to have obtained the web address for "Website A" directly from another source, such as other users of "Website A," or from online postings describing both the sort of content available on "Website A" and its

Internet, however, use of those gateways does not provide users with the full anonymizing benefits of the Network.

³ Due to a misconfiguration, prior to February 20, 2015, Website A was occasionally accessible through the traditional Internet. In order to access Website A in that manner, however, a user would have had to know the exact IP address of the computer server that hosted Website A, which information was not publicly available. As of on or about February 20, 2015, Website A was no longer accessible through the traditional Internet.

location. Accessing “Website A” therefore required numerous affirmative steps by the user, making it extremely unlikely that any user could

7. The Network’s software protects users’ privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user’s actual IP address which could otherwise be used to identify a user.

8. The Network also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within the Network itself, entire websites can be set up that operate the same as regular public websites with one critical exception - the IP address for the web server is hidden and instead is replaced with a Network-based web address. A user can only reach such sites if the user is using the Network client and operating in the Network. Because neither a user nor law enforcement can identify the actual IP address of the web server, it is not possible to determine through public lookups where the computer that hosts the website is located. Accordingly, it is not possible to obtain data detailing the activities of the users from the website server through public lookups.

Description of “Website A” and its Content

9. “Website A” was a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters

pertinent to the sexual abuse of children, including the safety and security of individuals who seek to sexually exploit children online. On or about February 20, 2015, the computer server hosting "Website A" was seized from a web-hosting facility in Lenoir, North Carolina. The website operated in Newington, Virginia, from February 20, 2015, until March 4, 2015, at which time "Website A" ceased to operate. Between February 20, 2015, and March 4, 2015, law enforcement agents acting pursuant to an order of the United States District Court for the Eastern District of Virginia monitored electronic communications of users of "Website A." Before, during, and after its seizure by law enforcement, law enforcement agents viewed, examined and documented the contents of "Website A," which are described below.

10. According to statistics posted on the site, "Website A" contained a total of 117,773 posts, 10,622 total topics, and 214,898 total members as of March 4, 2015. The website appeared to have been operating since approximately August 2014, which is when the first post was made on the message board. On the main page of the site, located to either side of the site name, were two images depicting partially clothed prepubescent girls with their legs spread apart, along with the text underneath stating, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." Based on my training and experience, I know that: "no cross-board reposts" refers to a prohibition against material that is posted on other websites from being "re-posted" to "Website A;" and ".7z" refers to a preferred method of compressing large files or sets of files for distribution. Two data-entry fields with a corresponding "Login" button were located to the right of the site name. Located below the aforementioned items was the message, "Warning! Only registered members are

allowed to access the section. Please login below or 'register an account' [(a hyperlink to the registration page)] with "[Website A]."

11. Upon accessing the "register an account" hyperlink, there was a message that informed users that the forum required new users to enter an email address that looks to be valid. However, the message instructed members not to enter a real email address. The message further stated that once a user registered (by selecting a user name and password), the user would be able to fill out a detailed profile. The message went on to warn the user, "[F]or your security you should not post information here that can be used to identify you." The message further detailed rules for the forum and provided other recommendations on how to hide the user's identity for the user's own security.

12. After accepting the above terms, registration to the message board then required a user to enter a username, password, and e-mail account; although a valid e-mail account was not required as described above.

13. After successfully registering and logging into the site, the user could access any number of sections, forums, and sub-forums. Some of the sections, forums, and sub-forums available to users included: (a) How to; (b) General Discussion; (c) [Website A] information and rules; and (d) Security & Technology discussion. Additional sections, forums, and sub-forums included (a) Jailbait – Boy; (b) Jailbait – Girl; (c) Preteen – Boy; (d) Preteen – Girl; (e) Pre-teen Videos – Girl HC; (f) Pre-teen Videos – Boys HC; (g) Toddlers; and (h) Kinky

Fetish – Scat. Based on my training and experience, I know that “jailbait” refers to underage but post-pubescent minors; the abbreviation “HC” means hardcore (i.e., depictions of penetrative sexually explicit conduct); and “scat” refers to the use of feces in various sexual acts, watching someone defecating, or simply seeing the feces. An additional section and forum was also listed in which members could exchange usernames on a Network-based instant messaging service that I know, based upon my training and experience, to be commonly used by subjects engaged in the online sexual exploitation of children.

14. A review of the various topics within the above forums revealed each topic contained a title, the author, the number of replies, the number of views, and the last post. The “last post” section of a particular topic included the date and time of the most recent posting to that thread, as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included in the post thread below it. Typical posts appeared to contain text, images, thumbnail-sized previews of images, compressed files (such as Roshal Archive files, commonly referred to as “.rar” files, which are used to store and distribute multiple files within a single file), links to external sites, or replies to previous posts.

15. A review of the various topics within the “[Website A] information and rules,” “How to,” “General Discussion,” and “Security & Technology discussion” forums revealed that the majority contained general information in regards to the site, instructions and rules for how to post, and welcome messages between users.

16. A review of topics within the remaining forums revealed the majority contained discussions about, and numerous images that appeared to depict, child pornography and child erotica depicting prepubescent girls, boys, and toddlers. Examples of these are as follows:

(a) On February 3, 2015, a user posted a topic entitled “Buratino-06” in the forum “Pre-teen – Videos - Girls HC” that contained numerous images depicting child pornography of a prepubescent or early pubescent girl. One of these images depicted the girl being orally penetrated by the penis of a naked male;

(b) On January 30, 2015, a user posted a topic entitled “Sammy” in the forum “Pre-teen – Photos – Girls” that contained hundreds of images depicting child pornography of a prepubescent girl. One of these images depicted the female being orally penetrated by the penis of a male; and

(c) On September 16, 2014, a user posted a topic entitled “9yo Niece - Horse.mpg” in the “Pre-teen Videos - Girls HC” forum that contained four images depicting child pornography of a prepubescent girl and a hyperlink to an external website that contained a video file depicting what appeared to be the same prepubescent girl. Among other things, the video depicted the prepubescent female, who was naked from the waist down with her vagina and anus exposed, lying or sitting on top of a naked adult male, whose penis was penetrating her anus.

17. A list of members, which was accessible after registering for an account, revealed that approximately 100 users made at least 100 posts to one or more of the forums. Approximately 31 of these users made at least 300 posts. In total, “Website A” contained thousands of postings and messages containing child pornography images. Those images included depictions of nude prepubescent minors lasciviously exposing their genitals or engaged in sexually explicit conduct with adults or other children.

18. “Website A” also included a feature referred to as “[Website A] Image Hosting.” This feature of “Website A” allowed users of “Website A” to upload links to

images of child pornography that are accessible to all registered users of “Website A.” On February 12, 2015, an FBI Agent accessed a post on “Website A” titled “Giselita,” which was created by a particular “Website A” user. The post contained links to images stored on “[Website A] Image Hosting.” The images depicted a prepubescent girl in various states of undress. Some images were focused on the nude genitals of a prepubescent girl. Some images depicted an adult male's penis partially penetrating the vagina of a prepubescent girl.

19. Text sections of “Website A” provided forums for discussion of methods and tactics to use to perpetrate child sexual abuse. For example, on January 8, 2015, a user posted a topic entitled “should i proceed?” in the forum “Stories - Non-Fiction” that contained a detailed accounting of an alleged encounter between the user and a 5-year-old girl. The user wrote “...it felt amazing feeling her hand touch my dick even if it was through blankets and my pajama bottoms...” The user ended his post with the question, “should I try to proceed?” and further stated that the girl “seemed really interested and was smiling a lot when she felt my cock.” A different user replied to the post and stated, “...let her see the bulge or even let her feel you up...you don't know how she might react, at this stage it has to be very playful...”

Court Authorized Use of Network Investigative Technique

20. Websites generally have Internet Protocol (“IP”) address logs that can be used to locate and identify the site’s users. In such cases, after the seizure of a website whose users were engaging in unlawful activity, law enforcement could review those logs in order to determine the IP addresses used by users of “Website A” to access the site. A publicly

available lookup could then be performed to determine what Internet Service Provider (“ISP”) owned the target IP address. A subpoena could then be sent to that ISP to determine the user to which the IP address was assigned at a given date and time.

21. However, because of the Network software utilized by “Website A,” any such logs of user activity would contain only the IP addresses of the last computer through which the communications of “Website A” users were routed before the communications reached their destinations. The last computer is not the actual user who sent the communication or request for information, and it is not possible to trace such communications back through the Network to that actual user. Such IP address logs therefore could not be used to locate and identify users of “Website A.”

22. Accordingly, on February 20, 2015, the same date “Website A” was seized, the United States District Court for the Eastern District of Virginia authorized a search warrant to allow law enforcement agents to deploy a Network Investigative Technique (“NIT”) on “Website A” in an attempt to identify the actual IP addresses and other identifying information of computers used to access “Website A.” Pursuant to that authorization, between February 20, 2015, and approximately March 4, 2015, each time any user or administrator logged into “Website A” by entering a username and password, the FBI was authorized to deploy the NIT, which would send one or more communications to the user’s computer. Those communications were designed to cause the receiving computer to deliver to a computer known to or controlled by the government data that would help identify the

computer, its location, other information about the computer, and the user of the computer accessing “Website A.” That data included: the computer’s actual IP address, and the date and time that the NIT determined what that IP address was; a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other computers; the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86); information about whether the NIT had already been delivered to the computer; the computer’s Host Name; the computer’s active operating system username; and the computer’s MAC address.

“pantyhosepedo” (Target in the WDNY) on “Website A”

23. According to data obtained from logs on “Website A,” monitoring by law enforcement and the deployment of a NIT, a user with the user name “pantyhosepedo” engaged in the following activity on “Website A.”

24. The profile page of user “pantyhosepedo” indicated this user originally registered an account on “Website A” on January 6, 2015. Profile information on “Website A” may include contact information and other information that is supplied by the user. It also contains information about that user’s participation on the site, including statistical information about the user’s posts to the site and a categorization of those posts. According to the “pantyhosepedo” profile, this user was a “Newbie” Member of “Website A.” Furthermore, according to the Statistics section of this user’s profile on “Website A,” the user

“pantyhosepedo” had been actively logged into the website for a total of 31 hours between the dates of January 6, 2015 and March 5, 2015.

25. According to the statistics on the “pantyhosepedo” profile page, between January 6, 2015, and March 5, 2015, this user made a total of 1 posting to “Website A.” On January 19, 2015, the user “pantyhosepedo” made a post replying to a post entitled “Valya in black bodystocking v33 – cut” in the “Panties, nylons, spandex” forum. This post he replied to contained 1 image of a girl wearing panty hose. She is sitting on what appeared to be a bed and is spreading her legs exposing her vaginal area to the camera.

IP Address and Identification of User “pantyhosepedo” on “Website A”

26. According to data obtained from logs on “Website A,” monitoring by law enforcement, and the deployment of a NIT, on February 25, 2015, the user “pantyhosepedo” engaged in the following activity on “Website A” from IP address 70.195.130.243. During the session described below, this user browsed “Website A” after logging into “Website A” with a username and a password.

27. On February 25, 2015, the user “pantyhosepedo,” with IP address 70.195.130.243, accessed the post entitled “ALD girl (all 11 vids).” Among other things, this post contained links to preview images as well as links to download the full files and the password to extract the file after it is downloaded. At the time agents viewed the content, none of the links were active.

28. An administrative subpoena was served upon Verizon Wireless (CellCo Partnership d/b/a Verizon Wireless) regarding IP address 70.195.130.243 on February 25, 2015, at 18:10 UTC associated with the user name “pantyhosepedo”. In response, Verizon Wireless provided a list of telephone numbers associated with the IP address 70.195.130.243. An examination of the list indicated that IP address 70.195.130.243 was used by the telephone number (716) 907-1608 on February 25, 2015, from 18:11 UTC to 18:45 UTC. A subsequent administrative subpoena was served upon Verizon Wireless for subscriber information relating to telephone number (716) 907-1608 from February 24, 2015, to February 26, 2015. The response from Verizon Wireless listed the “Account Name” as S. MALECKI.⁴ Public records and New York State Department of Motor Vehicles inquiries show S. MALECKI as a resident at what was later confirmed to be the defendant’s residence. The telephone number (716) 907-1608 is listed as the contact number for TROY MALECKI associated with utilities provided to the defendant’s residence.

29. During the following additional sessions, the user “pantyhosepedo” also browsed “Website A” after logging into “Website A” with a username and password. During these sessions, the user’s IP address information was not collected.

30. On or about February 25, 2015, the user “pantyhosepedo” viewed a thread entitled “Rainbow stats - Cute black girl sucks a big white dick” that contained a preview

⁴ The response from Verizon Wireless listed S. Malecki’s full name.

image, or contact sheet, with 16 images depicting what appears to be a prepubescent girl touching an adult male's erect penis with her hands and her mouth.

31. On or about March 4, 2015, the user "pantyhosepedo" viewed a thread entitled "Two cute girls yelp as they get the tip of a dick" that contained a preview image, or contact sheet, with 15 images depicting two prepubescent girls being vaginally penetrated by an adult male's erect penis.

32. Using publicly available websites, FBI Special Agents were able to determine that the above IP Address was operated by the Internet Service Provider ("ISP") Time Warner Cable.

33. In March 2015, an administrative subpoena/summons was served to Time Warner Cable requesting information related to the user who was assigned to the above IP address. According to the information received from Time Warner Cable, S. Malecki is receiving Internet service at the address at the defendant's address, with an installation date of August 13, 2014. Internet service was current as of June 1, 2015 at the aforementioned premises.

34. Based on the information obtained during the investigation, a federal search warrant was issued for the defendant's residence, and on September 18, 2015, Agents from the Buffalo Division of the FBI along with Task Force Officers conducted a search of the

residence pursuant to the search warrant. As a part of the search, Agents seized several items, including an LG-VS980 Cellular Telephone S/N 990002590723209, manufactured in Korea. This item was forensically processed utilizing the Cellebrite UFED 4PC tool.

35. Coincident to the execution of the search warrant, MALECKI was interviewed and admitted that he had been using the TOR network to access child pornography and viewed it numerous times. MALECKI stated that he masturbated to the content, and has struggled with this for about 20 years.

36. Your Affiant examined the report generated by the Cellebrite UFED 4PC tool for the following item: LG-VS980 Cellular Telephone S/N 990002590723209. A review of the results by your Affiant resulted in the discovery of more than 850 image files that contain child pornography as defined in Title 18 U.S.C. 2256. Listed below is the description of one of these image files, which I believe, based on my training and experience, constitutes child pornography:

a. **9183CBA867031FDC49FCF8D37CEE0C11EB2FE8AA.jpg** - this image file is a preview image, or contact sheet, with 13 images depicting what appear to be a nude female infant and a topless teenage female. The first four images show the infant being vaginally and anally penetrated with an object by the teenage female. The last nine images show the teenage female tying the infant's ankles to a long rod and then hanging the infant upside down. The

teenage female is also attaching clothes pins to the infant's nipples and vagina area. In the last five images, duct tape is covering the infant's mouth.

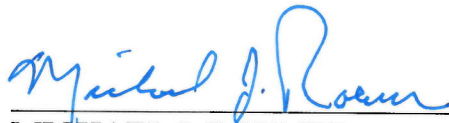
37. Based upon the foregoing, I respectfully submit that there is probable cause to believe that **TROY MALECKI** has violated Title 18, United States Code, Section 2252A(a)(5)(B).



S. R. Miller, Special Agent
Federal Bureau of Investigation

Sworn to before me this 26th

day of September, 2016.



MICHAEL J. ROEMER
UNITED STATES MAGISTRATE JUDGE